TRUDI

SUL PROC. DEL MASS. COMUN DIVISORE

TRA DUE FUNZ. INTERE DI UNA VARIABILE

SUL PROCESSO DEL MASSIMO COMUN DIVISORE

TRA DUE FUNZIONI INTERE DI UNA VARIABILE

NOTA

PER

N. TRUDI

Quasi tutti gli scrittori di algebra de' tempi nostri nel trattare dell'eliminazione tra due equazioni si rivolgono al metodo del massimo comun divisore, il quale ha infatti de'pregi teorici, che lo richiamano naturalmente nella teoria della eliminazione; ma la cosa va bene altrimenti nella pratica. Noi quì non staremo a ricordare gl'inconvenienti che accompagnano questo metodo, val dire la introduzione de'fattori estranei, che fan due mali ad un tempo, complicando i calcoli, ed i risultamenti finali. Quindi è che gli scrittori di quei libri, non esclusi alcuni de'più recenti, si sforzano di mostrare come debba ovviarsi a tali difetti; ma le son queste intenzioni eccellenti, cui non risponde il successo; dappoichè, messi da banda gli esempii all'uopo apparecchiati, le difficoltà restano intere. Ed infatti si può giudicare a priori della insufficienza dei mezzi, che si sogliono proscrivere, riflettendo alla loro assoluta inutilità per le equazioni letterali.

Ma questi scrittori hanno ormai l'obbligo di conoscere che i difetti di cui si tratta, sono da più tempo scomparsi per opera di uomini superiori, ed in particolare del Sylvester e del Brioschi; a che ci sia lecito di aggiungere una parte di perfezionamento, piccola come siasi, da noi recata a tal soggetto. (V. la nostra teoria de' determinanti). Così ora non solo è messa in piena luce la natura e la composizione di quei fattori estranei ma si formano e si scrivono all'istante i successivi residui,

indipendentemente gli uni dagli altri, sgombri da tutto ciò che ad essi non appartiene.

Dobbiamo aggiugnere tuttavia che tra gli algebristi Francoeur è, per quanto pare, il solo che abbia veduto nel suo vero aspetto il nodo della quistione, mentre è il solo, il quale esplicitamente dichiara (alg. sup. n.° 525) che « se si applica a due funzioni intere di una variabile il pro« cedimento del massimo comun divisore, o si operi in guisa da ottenere « residui interi non solo rispetto alla variabile, ma anche rispetto ai coef« ficienti, ogni resto, a cominciare dal secondo, è divisibile pel fattore « che conviene introdurre nella precedente divisione ad oggetto di evi« tare risultamenti frazionarii ».

Sono già molti anni che noi cercavamo a dimostrare le formole proposte dal Sylvester per esprimere in funzione delle radici di un'equazione i successivi residui, che si ottengono applicandole il teorema di Sturm, e non tardammo a riconoscere che queste formole aveano un intimo legame con la proposizione quì sopra enunciata del Francoeur; ma vedemmo nel tempo stesso che il ragionamento col quale è stabilita dal Geometra francese era assolutamente insufficiente. Noi quindi ci studiammo innanzi tutto ad assicurare di una maniera rigorosa questa proposizione, la quale era già per se stessa importante; ma non ebbimo per ciò a durar fatica, mentre potemmo assai presto riconoscere ch'essa era una conseguenza molto semplice di notissime proprietà delle successive derivate delle funzioni intere. Ora è per lo appunto la dimostrazione diretta di questa proposizione che presentiamo in questa nota, perchè serva come di compimento alla teorica del massimo comun divisore.

È nostro obbligo intanto di osservare che la stessa proposizione serve pure di fondamento agli estesi lavori del Sylvester sul medesimo soggetto, pubblicati fin dal 1853 nelle Transazioni Filosofiche; e pare senza dubbio che la insufficienza della dimostrazione del Francoeur abbia pure indotto il geometra inglese a cercarne da sua parte una dimostrazione, che dà infatti nell'art. 3° della 1ª parte della sua memoria; ma quantunque egli limiti il ragionamento a due funzioni, i di cui gradi differiscono di una unità, dobbiamo ingenuamente confessare di non avercene saputo rendere un conto esatto. E pare che l'autore istesso partecipi a questa incertezza, dappoichè, oltre alla dimostrazione, ha poi creduto di soggiungere una verifica, la quale non solo si rapporta al caso in cui i gradi delle due funzioni differiscono di *uno*, ma si limita a comprovare

che il solo principale cofficiente del secondo residuo è divisibile pel fattore introdotto nella prima divisione nello intento di evitar frazioni, dovendo poi ammettersi che avvenga altrettanto per tutti gli altri coefficienti.

Ciò premesso indicando con A e con B due funzioni intere, le più generali di gradi m ed n, sia

$$A = ax^m + a_1 x^{m-1} + a_2 x^{m-2} + \ldots + a_m,$$
$$B = bx^n + b_1 x^{n-1} + b_2 x^{n-2} + \ldots + b_n.$$

Se si applica a queste due funzioni il processo del massimo comun divisore, le operazioni possono essere regolate in guisa che i quozienti ed i resti siano interi non solo rispetto ad x, ma anche rispetto a tutte le altre lettere. Supposto $m>n$, sarà A il primo dividendo, B il divisore, ed il quoziente sarà una funzione intera di grado $m-n$, la quale adunque conterrà $m-n+1$ termini, nascenti da altrettante divisioni parziali, in cui il divisore è sempre il primo termine di B, cioè bx^n. Quindi, affinchè il quoziente riesca intero rispetto a tutte le lettere, basterà moltiplicare il dividendo A per la potenza di grado $m-n+1$ del coefficiente del primo termine del divisore B, vale a dire per b^{m-n+1}; ed allora anche il resto sarà intero rispetto a tutte le lettere, che figurano nelle due funzioni. Siccome questo resto è, in generale, una funzione di grado $n-1$, è chiaro che, a cominciare dalla seconda divisione il grado del dividendo sorpasserà di una unità il grado del divisore; e perciò, volendo che i quozienti ed i resti siano sempre interi a riguardo di tutte le lettere, bisognerà moltiplicare ogni dividendo pel quadrato del coefficiente del primo termine del corrispondente divisore.

Poichè i gradi de' resti, a cominciar dal primo, decrescono nell'ordine naturale da $n-1$ fino a *zero*, risulta che il numero di questi resti, e perciò anche il numero delle divisioni, e quello de' quozienti è, in generale, uguale ad n.

Posto ciò, supponendo istituito tra le date funzioni il processo del massimo comune divisore, e regolate le operazioni nel modo già detto affin di avere quozienti e resti interi rispetto alla variabile ed alle costanti, andremo a dimostrare, che:

Ogni resto, a cominciare dal secondo, è esattamente divisibile pel fattore introdotto nella precedente divisione ad oggetto di evitar frazioni.

Dimostr. Siano Q_1, ed R_1, il quoziente ed il resto della divisione di $b^{m-n+1}A$ per B; sia inoltre c il coefficiente della più alta potenza di x in R_1; e siano infine Q_2 ed R_2 il quoziente ed il resto della divisione di c^2B per R_1. Così, se pongasi

$$s=m-n+1\ ,$$

per la natura della divisione si avranno le due identità

$$b^sA=Q_1B+R_1\ ,$$
$$c^2B=Q_2R_1+R_2\ ,$$

dalle quali, eliminando R_1, e messo per compendio

$$y=c^2+Q_1Q_2\ ,$$

si ha l'altra

$$R_2=yB-b^sQ_2A\ . \qquad (1)$$

Facendovi $b=o$, si ha per immediata riduzione

$$R_2=yB\ ;$$

ma si comprende che questa formola è ancora suscettibile di altre riduzioni, poichè in generale le quantità R_2, y, B contengon tutte la costante b. Però, quali che siano queste riduzioni, è evidente che il grado di R_2 è sempre minore del grado del prodotto yB; dappoichè la ipotesi di $b=o$ non fa che privare il polinomio B del solo primo termine bx^n; e perciò il prodotto è per lo meno di grado $n-1$, mentre il grado di R_2 non può essere superiore ad $n-2$. Segue da ciò che, per $b=o$, le due quantità R_2 ed yB debbono identicamente annullarsi; ma in riguardo al prodotto yB è da osservare che, non potendo annullarsi il fattore B, è il fattore y quello che si annulla. Riguardo poi ad R_2, siccome questa quantità si annulla nella ipotesi di $b=o$, ciò dimostra ch'essa è divisibile per b; ma resta a trovare il grado di moltiplicità di questo fattore.

A tale oggetto noi considereremo le successive derivate dall'eguaglianza (1) rispetto a b; ed innanzi tutto osserveremo, 1°: che la derivata di B è x^n; 2°; che dalla prima derivata fino a quella dell'ordine $s-1$, inclusivo, i termini provvenienti dal prodotto b^sQ_2A sono tutti af-

fetti dal fattore b; mentre da quella dell'ordine ε in poi vi sarà sempre un termine indipendente da b. Quindi, se nelle successive derivate della (1), prese rispetto a b, si faccia $b=o$, le prime $\varepsilon-1$ derivate del secondo membro debbono ridursi ai soli termini provvenienti dal prodotto yB; e perciò nella detta ipotesi si hanno le seguenti $\varepsilon-1$ identità: (*)

$$R'_2=y'\,B+\ yx^n\ ,$$
$$R''_2=y''\,B+2y'x^n\ ,$$
$$R'''_2=y'''\,B+3y''x^n\ ,$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$
$$R^{(\varepsilon-1)}_2=y^{(\varepsilon-1)}B+(\varepsilon-1)\,y^{(\varepsilon-2)}x^n\ .$$

Ora si è dimostrato poc'anzi che per $b=o$ si ha $y=o$; dunque la prima identità si riduce ad $R'_2=y'B$; ma quindi per la necessaria diversità di gradi de' due membri si conchiuderà come prima che debba essere ad un tempo $R'_2=o$ ed $y'=o$. Ma, così essendo, la seconda identità diviene $R''_2=y''B$, e porge per la stessa ragione $R''_2=o$ ed $y''=o$. Similmente si otterrebbe dalla terza $R'''_2=o$ ed $y'''=o$. Ma ora senza più è palese che l'ipotesi di $b=o$, mentre annulla il secondo residuo R_2, annulla contemporaneamente le sue successive derivate rispetto a b, fino a quella dell'ordine $\varepsilon-1$; e ne risulta che questo residuo è divisibile per b^ε, ossia per b^{m-n+1}, ch'è il fattore introdotto nella precedente divisione ad oggetto di evitar frazioni. Ora è chiaro che il teorema resta con ciò compiutamente dimostrato, mentre l'ultima conchiusione è applicabile a qualunque altra divisione, osservando che ogni resto, a cominciar da terzo, sarà divisibile pel quadrato del coefficiente della più alta potenza del resto precedente.

Segue da questo teorema che il processo del massimo comun divisore tra le due funzioni A e B si può condurre innanzi sotto due condizioni:

1°, che i resti siano interi rispetto a tutte le lettere:

2°, che ogni resto, prima di prendersi per divisore, sia spogliato dal fattore, dal quale è affetto in virtù del teorema.

Noi, col Sylvester, distingueremo i residui ottenuti in tal guisa con l'epiteto di *semplificati*, mentre possono chiamarsi residui *completi* quelli

(*) In queste formole gli apici sono indici di *derivazione*.

che si otterrebbero eseguendo le operazioni del massimo comun divisore, senza sopprimere, nè introdurre alcun fattore. Ora ben si comprende che i residui utili in tutte le teoriche di analisi, alle quali suole applicarsi il processo del massimo comun divisore, sono i residui semplificati, e vede ognuno di quale importanza è un metodo che permettesse di ottenerli di una maniera semplice e spedita. Questo metodo intanto è già conosciuto; esso è fondato sulla teorica de' determinanti (v. il nostro trattato di queste funzioni), e costituisce indubitatamente un progresso dell'analisi algebrica. Quì tuttavolta dobbiamo osservare la impossibilità assoluta di raggiungere cosiffatti risultamenti per le vie ordinarie della divisione; e ciò solo basterebbe a provare che i determinanti son tutto altro che usate cognizioni, circondate di nuovi nomi.

Porremo termine a questo articolo dimostrando una proprietà de' semplificati residui di molto interesse per le applicazioni. Ponendo mente alla notazione adottata per le funzioni A e B, e ritenuto che i coefficienti a e b delle loro più alte potenze siano affetti dall'indice *zero*, sarà lecito di riguardarle come funzioni omogenee in rapporto agli esponenti della variabile ed agl'indici delle costanti; e sotto questo aspetto sarà m il grado di omogeneità di A, ed n quello di B. Quindi anche omogenei saranno i resti delle divisioni; ma è importante di determinare con precisione il grado di omogeneità di ciascuno di essi.

Siano $r_1, r_2, r_3, \ldots, r_s$ i primi s semplificati residui; $c_1, c_2, c_3, \ldots, c_s$ i coefficienti de' loro primi termini, e $q_1, q_2, q_3, \ldots, q_s$ i corrispondenti quozienti. Così le s divisioni daranno luogo alle seguenti s equazioni identiche ed omogenee;

$$b^2 A = q_1 B + r_1 \quad ,$$

$$c_1^2 B = q_2 r_1 + b^2 r_2 \; ,$$

$$c_2^2 r_1 = q_3 r_2 + c_1^2 r_3 \; ,$$

$$c_3^2 r_2 = q_4 r_3 + c_2^2 r_4 \; ,$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \; ,$$

$$c_{s-1}^2 r_{s-2} = q_s r_{s-1} + c_{s-2}^2 r_s \; .$$

e però i gradi di omogeneità de' loro ultimi tèrmini saranno uguali a quelli de' loro primi membri. In conseguenza, se si dinotano con g_1, $g_2, \ldots, g_s$ i gradi di omogeneità de' resti $r_1, r_2, \ldots, r_s$, e siano g'_1, g'_2,

..., g'_s quelli de'loro primi coefficienti c_1, c_2, ..., c_s, si avranno le seguenti s relazioni

$$
\begin{aligned}
g_1 &= m \quad ,\\
g_2 &= n \quad + 2g'_1 \quad ,\\
2g'_1 \quad + g_3 &= g_2 \quad + 2g'_2 \quad ,\\
2g'_2 \quad + g_4 &= g_3 \quad + 2g'_3 \quad ,\\
2g'_3 \quad + g_5 &= g_4 \quad + 2g'_4 \quad ,\\
\ldots \quad &\ldots \quad ,\\
2g'_{s-2} + g_s &= g_{s-1} + 2g'_{s-1} \quad ,
\end{aligned}
$$

le quali addizionate membro a membro porgono

$$g_{s-1} + g_s = m + n + 2g'_{s-1} \ .$$

D'altra parte, siccome g_{s-1} e g_s, gradi di omogeneità do'resti r_{s-1} ed r_s, sono rispettivamente uguali a'gradi di omogeneità de'loro primi termini $c_{s-1}x^{n-s+1}$ e $c_s x^{n-s}$, si ha

$$
\begin{aligned}
g_{s-1} &= g'_{s-1} + n - s + 1 \ ,\\
g_s \quad &= g'_s \quad + n - s \quad ,
\end{aligned}
$$

e quindi addizionando

$$g_{s-1} + g_s = 2n - 2s + 1 + g'_{s-1} + g'_s \ .$$

Così, paragonando questa relaziono con la precedente si ottiene

$$g'_s = (m - n - 1) + 2s + g'_{s-1} \ .$$

Questa formola, facendovi successivamente $s=1$, 2, 3, .., s, ed osservando che $g_0=0$, conduce allo relazioni

$$
\begin{aligned}
g'_1 &= (m-n-1) + 2 \, . \, 1\\
g'_2 &= (m-n-1) + 2 \, . \, 2 + g'_1\\
g'_3 &= (m-n-1) + 2 \, . \, 3 + g'_2\\
g'_4 &= (m-n-1) + 2 \, . \, 4 + g'_3\\
\ldots &\ldots\\
g'_s &= (m-n-1) + 2 \, . \, s + g'_{s-1} \ ,
\end{aligned}
$$

le quali addizionate danno

$$g'_s = s(m-n-1) + s(s+1) \ ,$$

ossia

$$g'_s = s(m-n+s) \ ;$$

e siccome $g_s = g'_s + n - s$, così risulta infine

$$g_s = s(m-n-1+s) + n \ .$$

Con questa formola adunque si può valutare il grado di omogeneità di un residuo qualunque r_s in rapporto agli esponenti della variabile, ed agl'indici delle costanti. Se si tratta dell'ultimo residuo r_n, si ha

$$g_n = mn \ ,$$

e si ha pure

$$g'_n = mn \ ;$$

Ma in questo caso l'eguaglianza de' valori di g_n e g'_n era bene da prevedersi, poichè l'ultimo residuo r_n è una funzione di grado *zero*, cioè una costante; e quindi g_n e g'_n significano una stessa cosa. Per tanto gli ultimi risultamenti dimostrano che il grado di omogeneità dell'ultimo semplificato residuo r_n è uguale al prodotto de' gradi delle date funzioni A e B; il che coincide col noto teorema relativo alla dimensione delle risultanti delle due equazioni $A=0$ e $B=0$.